

Job Opening: Security Operation Center Analyst

Join us and kick-start your career in IT-security!

We currently have an exciting opportunity to join the Managed Security Services (MSS) team as a Security Operations Centre Analyst.

The Team: Managed Security Services (MSS) is composed of several teams: our two Ottawa 24x7x365 Security Operations Centres (SOCs), the Deployment and Support teams (5 teams which are each focused on several technologies and services), the solution architects, the project managers, and the client service managers. We are a very collaborative close-knit team in MSS – team spirit and satisfying career growth for our members are a key focus for all of us.

Why us: CGI does consulting, yes, but our team is different. MSS is a dynamic and stable team of 80 security professionals working together since 2001. We are growing! Come join us and see what it's like to work and learn in the exciting field of IT security with a great group of professionals. The SOC seniors and the members of the other MSS teams are supportive and collaborative – you'll have the support you need to be successful in your position and to grow your security skills and career.

Career growth: This role provides excellent career growth potential since you will be learning leading-edge technologies and methodologies, have access to our various training options and there are multiple career growth paths within the MSS Team. If you are serious about growing your skills and career, we're serious about giving you the opportunities to grow and learn multiple security technologies and standards or to take on other tasks that are of interest to you beyond what is listed above.

Technical environment: We use top-ranked industry-leading security tools and technologies – several security technologies for each of our multiple services. MSS has an on-site lab which all our members can use for installation trials and proof-of-concepts, training, testing and trouble-shooting.

Our Clients: Many large big-name clients trust our team and use our many managed security services to protect their business. We are gaining many new clients and the list has been growing globally into Europe and Asia since CGI's acquisition of Logica.

Your future duties and responsibilities

The Opportunity: The Security Operations Centre Analyst will, after an extensive training period and with ongoing support:

- Monitor security alerts of potential hacker attacks detected by security systems such as: Intrusion Detection & Prevention Systems (NIDS/NIPS, HIDS/HIPS, WIDS), Log Monitoring, File Integrity Monitoring and SIEM.
- Determine and classify the severity of alerts and assess potential impacts.

- Report and investigate potential security incidents.
- Provide recommendations to clients for containment and eradication of threats.
- Maintain Intrusion Detection/Prevention signatures.
- Update security operations processes and procedures.
- Assist in IT security investigations, exercises and tests.

- Research, consultation with colleagues and training to maintain awareness of trends in new security threats, technologies and regulations.
- Other related duties as assigned by the supervisor.
- Since this is a 24x7x365 environment, shift work (rotation) is required. Many of our SOC team enjoy the flexibility this gives them in their life since they have 3 days on and three days off (12 hour shifts).

Required qualifications to be successful in this role

Experience and Education:

- Experience in IT (Information Technology) and an interest in IT Security.
- Understanding, and preferably some experience as well, of networking and TCP/IP.
- A non-mandatory asset would be completion of a post-secondary educational program in IT Security or Computer Sciences from a recognized community college or university.
- Government of Canada Secret Clearance is required (or the ability to obtain one)